Daniel Rigmaiden
Agency # 10966111
CCA-CADC
PO Box 6300
Florence, AZ 85132
Telephone: none
Email: none

Daniel David Rigmaiden
Pro Se, Defendant

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

United States of America, Plaintiff, v. Daniel David Rigmaiden, et al., Defendant.	No. CR08-814-PHX-DGC MOTION FOR RECONSIDERATION OF PORTIONS OF COURT'S ORDER AT Dkt. #1009 RE: FOURTH AMENDMENT SUPPRESSION ISSUES

Defendant, Daniel David Rigmaiden, appearing *pro se*, respectfully submits *Motion For Reconsideration Of Portions Of Court's Order At Dkt. #1009 RE: Fourth Amendment Suppression Issues*. LRCiv 7.2(g) states that a motion for reconsideration may be brought if there is "manifest error or a showing of new facts or legal authority that could not have been brought to its attention earlier with reasonable diligence. Any such motion shall point out with specificity the matters that the movant believes were overlooked or misapprehended by the Court, any new matters being brought to the Court's attention for the first time and the reasons they were not presented earlier, and any specific modifications being sought in the Court's Order." *Id*. The defendant separates this motion for reconsideration into three primary sections: (1) Manifest Errors of Fact, (2) Manifest Errors of Law, and (3) Modifications Of The Order Being Sought. All listed errors are manifest errors.[1] In light

1. Preparing a motion addressing all manifest errors of fact and law would take longer than the 14 days provided for in LRCiv 7.2(g)(2). Therefore, the defendant is only addressing some manifest errors.

of the manifest errors listed below, the defendant respectfully requests that the Court reevaluate the portions of its order referenced in Section III of this motion and modify its order accordingly.

This motion for reconsideration does not address the Court's denial of the defendant's motions at Dkt. #847 and Dkt. #927, which are currently being appealed (interlocutory) to the United States Court of Appeals for the Ninth Circuit.

I. Manifest Errors of Fact

1. *Manifest Factual Errors*: ***(a)*** Dkt. #1009, p. 5, ln. 6-8: "The rental application listed a fake California driver's license bearing a number *that belonged to a female with a different name*..."; ***(b)*** Dkt. #1009, p. 8, ln. 27-28: "Defendant provided a forged California driver's license in Brawner's name, along with a driver's license number *assigned to a living female*."; ***(c)*** Dkt. #1009, p. 9, ln. 1-6: "Defendant rented a storage unit using the identity of Daniel Aldrich, a deceased person, with a fraudulent driver's license number *assigned to another living person*. [] Defendant... used yet *another person's driver's license number* in connection with the Stout identification..."; ***(d)*** Note: this is only a sampling. The Court repeatedly noted how IDs used by the defendant had driver license numbers that did not correspond to the names on the IDs.;

Correction Supported By Evidence: Whenever there was an ID card from the evidence, the driver license number on the card was invented, *i.e.*, made up.[2] The defendant also made this clear in a prior declaration.[3] Therefore, the Court erroneously counted each ID card as two assumed identities. In other words, the Court counted each made-up driver license number as an additional so-called "fraudulent identity" entirely separate from any identity actually used by the defendant. Because the defendant could not have known that the made-up ID numbers actually belonged to other people, it was manifest

---

2. *See* defendant's Declaration RE: *Daniel Rigmaiden had no plans for a "quick escape" or "quick departure," made no "preparations to flee," was not ready to "abandon the apartment on a moment's notice," and did not maintain a storage unit as part of an "escape plan"*, p. 5-6, ¶ 12 (EXHIBIT 01).

3. *See* Dkt. #894-1, p. 1, ¶ 2 ("The driver license number... w[as a] **random number**[] following the established format for California ID numbers..." (emphasis added)).

error for the Court to engage in double counting during its hyperbole. *See* Flores-Figueroa v. United States, 129 S.Ct. 1886 (2009) (if defendant obtains fake ID card under his name but uses ID number of another person, government must prove he knew the ID number belonged to another person). In the present case, the government did not and cannot allege, let alone prove, prior knowledge regarding the made-up ID numbers on driver licenses. Therefore, while determining the defendant's reasonable expectation of privacy, the Court factually erred by counting each made-up ID number as an additional so-called "fraudulent identity" used by the defendant.

2. *Manifest Factual Errors*: ***(a)*** Dkt. #1009, p. 7, ln. 23-24: "It is also true, however, that Defendant was prepared to abandon the apartment on a moment's notice."; ***(b)*** Dkt. #1009, p. 8, ln. 7-10: "Given Defendant's preparations to flee and his admission that he would have done so had he learned of the government's investigation, it could be argued that Defendant had already formed an intent to abandon his aircard, computer, and apartment."; ***(c)*** Dkt. #1009, p. 34, ln. 19-20: "Defendant argues that he would have fled and never been found if the warrant had been served...";

Correction Supported By Evidence: First, the defendant never stated that he was prepared to abandon his apartment at all. The defendant had **no intent** and made **no preparations** to abandon his apartment.[4] He stated that he would **move**[5] after packing up his belongings and cleaning the apartment[6]—something a person does when properly ending a 10-month lease, not something someone does when "fleeing" as the Court fallaciously asserted in its order. Likewise, the defendant did not state that he would "flee on

---

4. *See* defendant's Declaration RE: *Daniel Rigmaiden had no plans for a "quick escape" or "quick departure," made no "preparations to flee," was not ready to "abandon the apartment on a moment's notice," and did not maintain a storage unit as part of an "escape plan"*, p. 1, ¶ 2 (EXHIBIT 01).

5. *See* Dkt. #824-1, p. 322 (Had the defendant been given notice that the government was violating his civil rights via the N.D.Cal. 08-90330MISC-RS, "within the 18 day period after the aircard had been located... the defendant would have... packed up his belongings and permanently **moved** from apartment No. 1122." (emphasis added)).

6. Dkt. #824-2, p. 4, ¶ 14 ("Had I received notice of the aircard locating mission, within a day I would have permanently left apartment No. 1122 after packing up my belongings and cleaning the apartment." (defendant's declaration)).

a moment's notice." The Court's assertion has no basis in fact and is unsupported by the record. The defendant made very clear in his declaration that he would have **moved within a day** after packing up his belongings and cleaning his apartment. One day is not a "moment's notice," but a reasonably estimated move out period considering the defendant's studio apartment was only 489 *ft²*.[7] In fact, this is more time than it would take most people to pack up and move from a 489 *ft²* space. The defendant calculated in extra time considering he had no car and had no driver license.[8]

Furthermore, the defendant never made an admission that he would flee "had he learned of the government's investigation." The Court's assertion has no basis in fact and is unsupported by the record. The defendant made very clear in his declaration that he would have **moved** within a day after packing up his belongings and cleaning his apartment *only if* he would have been served with a copy of the N.D.Cal. 08-90330MISC-RS order.[9] By being served with a copy of the unconstitutional order—which contains no details of the underlying investigation—the defendant would have only learned of the government violating his Fourth Amendment rights. Obviously a difficult concept for the Court and government to grasp, the defendant highly values his Constitutional rights and would have moved in order to prevent further degradation of those rights by overzealous government agents.[10] By moving, the defendant would have eliminated the poisonous fruits of the government's illegal search.[11] This is the same remedy (*i.e.*, the suppression remedy) used

---

7. *See First Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 29 (Dkt. #587-2) (Domicilio apartments floor plans showing studio apartment at 489 *ft²*); *id.*, EXHIBIT 30 (Dkt. #587-2) (Domicilio apartments site map showing apartment No. 1122 to be a studio apartment).

8. *See* defendant's Declaration RE: *Daniel Rigmaiden had no plans for a "quick escape" or "quick departure," made no "preparations to flee," was not ready to "abandon the apartment on a moment's notice," and did not maintain a storage unit as part of an "escape plan"*, p. 1, ¶ 2 (EXHIBIT 01).

9. *See* Dkt. #824-2, p. 4, ¶ 14.

10. *See* defendant's Declaration RE: *Daniel Rigmaiden had no plans for a "quick escape" or "quick departure," made no "preparations to flee," was not ready to "abandon the apartment on a moment's notice," and did not maintain a storage unit as part of an "escape plan"*, p. 2, ¶ 3 (EXHIBIT 01).

11. *See id*.

by courts when seeking to **alter** government activity so that it complies with the Fourth Amendment. It was then and it is now the defendant's belief that making such a stand against overzealous government activity is every citizen's right and duty.[12] The defendant's original declaration (Dkt. #824-2) contained no reason for the move and it was manifest error for the Court to make up its own reason and present it as fact.

The Court also claimed that "Defendant argues that he would have fled and never been found..." The Court's assertion has no basis in fact and is unsupported by the record. The defendant never claimed that he would have "fled and never been found." The defendant made clear in his reply brief that "there would have been nothing for the government to seize and nobody for the government to arrest **during the in-person search of apartment No. 1122 on August 3, 2008**."[13] Contrary to the Court's assessment, "forever" does not exist within the single, lone day of August 3, 2008. The defendant's point is clear: had he been served with a copy of the unconstitutional N.D.Cal. 08-90330MISC-RS order, the **August 3, 2008** "in-person search of apartment No. 1122 would have never produced evidence or the defendant[]"[14] because he would have "moved from apartment No. 1122 with all of his belongings before the government's execution of the N.D.Cal. 08-70460-HRL/PVT search warrant."[15] Whether the government would have followed the defendant to his new home or stopped him along the way is unknown. Whether a new search warrant for his new home would have been obtained and executed is unknown. The government submitted no scenarios for the Court to consider. What *is* clear is that the August 3, 2008 execution of the N.D.Cal. 08-70460-HRL/PVT search warrant would not have produced evidence had the government served the defendant with a copy of the N.D.Cal. 08-90330MISC-RS order. Nothing more, nothing less. The Court's hyperbole only

---

12. *See id.*; *see also United States Declaration of Independence* (Jul. 4, 1776) ("That whenever any Form of Government becomes destructive of these ends, it is the Right of the People to **alter**... it" (emphasis added)). Note: every act of protest in response to illegal government activity is an attempt to alter government.

13. Dkt. #824-2, p. 4, ¶ 14.

14. Dkt. #900, p. 44.

15. *Id.*

builds a fantasy.

3. *Manifest Factual Errors*: ***(a)*** Dkt. #1009, p. 8, ln. 3-7: "The government also asserted during oral argument, without contradiction from Defendant, that Defendant's rented storage unit was found to contain $70,000 in cash, a United States passport issued to Defendant in the name of Andrew Johnson (a deceased individual), and a computer with back-up information from Defendant's laptop, all apparently awaiting a quick departure."; ***(b)*** Dkt. #1009, p. 9-8, ln. 27-28 & 1-2: "What's more, while living in the apartment under false pretenses, Defendant had $70,000 in cash, a false passport, and a copy of his laptop computer in a storage unit (also rented under false pretenses) ready for a quick escape.";

Correction Supported By Evidence: First, the purpose of the defendant maintaining a storage unit was simply for the storage of property.[16] The defendant did not maintain a storage unit to facilitate a quick departure. The government and Court's assertions to the contrary are ludicrous and entirely contrary to fact and truth.

Second, the defendant never agreed to the government's *assumption* that the items in the storage unit were there for a "quick departure" or "quick escape,"[17] as the Court fallaciously asserted in its order. The March 28, 2013 hearing was not an evidentiary hearing and the government presented no evidence that the defendant was required to rebut. Nevertheless, the government's claim made for the **first time** on March 28, 2013 was framed as an *assumption*, not a fact supported by evidence:

> I think it's a very safe **assumption** that if Mr. Rigmaiden wanted to drop out of sight and change identities, he could have done it instantaneously. We know he could have done that, because when we executed the search warrant for the storage unit, we found a facially valid U.S. passport in the name of Johnson... He had over $70,000 in cash... and, oh, by the way, a backup computer with all of his information...
>
> *March 28, 2013 Motion Hearing Transcript*, [MR BATTISTA], p. 86-87 (emphasis added).

---

16. *See* defendant's Declaration RE: *Daniel Rigmaiden had no plans for a "quick escape" or "quick departure," made no "preparations to flee," was not ready to "abandon the apartment on a moment's notice," and did not maintain a storage unit as part of an "escape plan"*, p. 3-4, ¶ 6 (EXHIBIT 01).

17. *See id.*, p. 4, ¶ 7 (EXHIBIT 01).

Third, there was no computer in the storage unit as assumed by the government.[18] The items that were seized from the storage unit are listed in the return on the record at Dkt. #846-3. As the return shows, there was no computer or laptop in the storage unit.

Fourth, not only did the defendant have no plans for a "quick escape," he could not have made a "quick escape" considering he did not own a car and had no driver license.[19] This is why the defendant indicated in his earlier declaration that it would take him "a day" to move from his apartment after cleaning it—hardly a "quick escape."

Fifth, the government failed to present any evidence that the storage unit was part of a plan for a "quick escape." For example, the government presented no statements by the defendant, and no files or emails from the defendant's home computer detailing an escape plan involving the storage unit or any escape plan for that matter. Agents have been searching through the defendant's data for 3+ years and found no such evidence. This is why the government framed its statement at the March 28, 2013 motions hearing as an *assumption*, not a *fact*.

Sixth, the storage unit records and the combination to the lock for the storage unit was found in the defendant's apartment during the August 3, 2008 search.[20][21] It does not logically follow that a person would keep the combination and rental records of a storage unit at the very location he planned to "escape" from. In addition to having no basis in fact, the Court and government's assertions have no basis in common sense.

4. *Manifest Factual Errors*: ***(a)*** Dkt. #1009, p. 8, ln. 13-14: "Defendant purchased the aircard in May of 2006 using the name of a living person, Travis Rupard.";

Correction Supported By Evidence: The defendant did not purchase the aircard using the name of Travis Rupard. This point was reiterated in numerous briefs and other documents that have been on the record for months. As the defendant's declaration states, he

18. *See id.*, p. 4, ¶ 8 (EXHIBIT 01).

19. *See id.*, p. 4, ¶ 9 (EXHIBIT 01).

20. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 05 (Dkt. #863-1) (explaining how a text file seized from apartment No. 1122 documented the rental of the storage unit).

21. *See id.*, p. 4, ¶ 10 (EXHIBIT 01).

purchased his aircard using cash without giving a name.[22] In fact, the defendant purchased several aircards in 2006 before deciding which one to activate after the purchases were made. It was manifest error for the Court to adopt the government's unsupported assertion over the defendant's uncontested declaration.

5. *Manifest Factual Errors*: ***(a)*** Dkt. #1009, p. 8, ln. 17-19: "He used a fraudulent Visa card in Johnson's name to purchase the computer, and procured the Visa card by using Johnson's Social Security Number."; ***(b)*** Dkt. #1009, p. 8, ln. 19-20: "The Ninth Circuit has held that a defendant does not have a reasonable expectation of privacy in computer equipment obtained through fraud.";

Correction Supported By Evidence: A recurring theme, the Court builds a straw man to better suit an application of Caymen, 404 F.3d 1196 (9th Cir. 2005) (defendant used a stolen credit card to purchase a computer). The Court presented the facts as if the defendant had used a fraudulent **credit** card to purchase his home computer; resulting in monetary loss to a victim. Contrary to the Court's straw man, the defendant purchased his computer using a "stored value card," *i.e.*, a prepaid debit card funded with his own money. The defendant's **uncontested** declaration states that he used a WiredPlastic card of which he purchased and funded himself[23]—not a credit card belonging to another person, as fallaciously asserted by the Court in its order. There is a crucial difference, *i.e.*, the "fraud" and "theft" factual elements present in *Caymen* are not present here.

6. *Manifest Factual Errors*: ***(a)*** Dkt. #1009, p. 10, ln. 18-20: The Court commented on the facts of Bautista, 362 F.3d 584 (9th Cir. 2004) in order to distinguish them from the facts of the present case. To distinguish the two cases and support a finding that the defendant had no reasonable expectation of privacy in his home, the Court noted the following about the search in *Bautista*: "Third, law enforcement officers conducted no investigation of the defendant's use of the stolen credit card before entering the room...";

Correction Supported By Evidence: In the present case, it is also a fact that the

22. *See* Dkt. #824-3, ¶ 2, p. 1.

23. *See* Dkt. #824-3, ¶ 4, p. 2-3.

government conducted no investigation into any of the so-called "fraud" of which the Court relied to support its finding that the defendant had no reasonable expectation of privacy in his home residence. The government knew nothing about the defendant's use of the Steven Brawner name to rent the apartment until after FBI technical agents had operated the StingRay to locate the apartment.

7. *Manifest Factual Errors*: ***(a)*** Dkt. #1009, p. 13, ln. 18-20: "The intrusion that allowed agents to locate the aircard – using a mobile tracking device to send signals to and receive signals from the aircard – was not a 'severe intrusion.'";

Correction Supported By Evidence: The government already conceded that "the aircard tracking operation was a Fourth Amendment search and seizure."[24] A Fourth Amendment search and seizure, by definition, is a "severe intrusion." Additionally, *see* Section II(B), *infra*, explaining how both the Court and government agreed to accept and not challenge the defendant's identification/classification of independent government actions into separate Fourth Amendment searches and seizures.

8. *Manifest Factual Errors*: ***(a)*** Dkt. #1009, p. 33, ln. 6-9: "Moreover, the warrant specifically required the government to 'expunge all of the data' at the conclusion of the tracking mission. [] The government explained that this was done precisely because the device captured information from cell phones and aircards unrelated to this investigation."; ***(b)*** Dkt. #1009, p. 31, ln. 16-19: "[T]he evidence presented by the government and Defendant shows that the third-party information was deleted from the mobile tracking device immediately after the aircard was located.";

Correction Supported By Evidence: The government's purpose for deleting all data gathered by the StingRay and KingFish was not to protect third-parties. If that was the case, the government would have still preserved the data relating specifically to the defendant's aircard. Additionally, if that was the case, the government would have immediately deleted the third-party data on July 17, 2008, after use of the equipment had concluded, rather than

24. *Government's Memorandum Re Motion For Discovery* (Dkt. #674, p. 1).

wait until after the defendant's arrest on August 3, 2008.[25] Clearly, deleting all data, including the evidence relating to the defendant's location, was done to hide details of the device from the defense. Additionally, the government had at least **18 days** to rummage through third-party data seized from third-party cell phones and aircards prior to deletion. The Court's claim that the third-party data and actual evidence in this case was deleted "immediately after the aircard was located" is just more fallaciousness and contradiction to prior findings.[26] The government did not have third-party privacy interests in mind.

9. *Manifest Factual Errors*: ***(a)*** Dkt. #1009, p. 48, ln. 18-20: "As the government argues, 'agents were using a relatively new technology, and they faced a lack of legal precedent regarding the proper form of a warrant to obtain the location information they sought.'";

Correction Supported By Evidence: It is common knowledge that the FBI has been using cell site emulators since the 1990s.[27] In February of 2009, one FBI agent testified that he alone used such equipment more than 300 times over the last nine years.[28] This was not "new" technology to the government in the year 2008. It was only "new" to countless judges—including the judge presiding over this case—who were kept in the dark for a number of years prior to the defendant exposing the government's warrantless and illegal use of the equipment.

10. *Manifest Factual Errors*: ***(a)*** Dkt. #1009, p. 16, ln. 3-4: "The data was produced to the government after being extracted by a Quality Alarm employee from access equipment at the complex."; ***(b)*** Dkt. #1009, p. 21 ln. 1-2: "The fact that this transaction

---

25. *See January 4, 2012 Court Order* (Dkt. #723, p. 14) (Noting the settled fact that "[a]ll data generated by the [][portable/transportable wireless device locators] and received from Verizon as part of the locating mission was destroyed by the government **shortly after Defendant's arrest on August 3, 2008**." (emphasis added)).

26. *See* fn. No. 25, *supra*.

27. *See* Shimomura, Tsutomu, *Catching Kevin* [Mitnick], 19**93**-2004 The Condé Nast Publications Inc., *available at* http://www.wired.com/wired/archive/4.02/catching_pr.html (last accessed: Apr. 5, 2012) ("The team talked to me a little about the technology they had toted along in the station wagon, especially something called a cell-site simulator, which was packed in a large travel case.").

28. *See* United States v. Allums, No. 2:08-CR-30 TS, District of Utah (Doc. #128, p. 16 and 43) (transcripts of testimony given by FBI Agent William Shute).

between Defendant and the alarm company was recorded in data retained by the alarm company would come as no surprise to anyone even passingly familiar with modern electronic systems.";

Correction Supported By Evidence: First, the Court failed to recognize that Quality Alarm Service assisted FBI Agent Richard J. Murray in *his* effort to physically seize the geolocation data from the physical readers at the Domicilio apartment complex. The subpoena was used as if it were a warrant executed by a federal agent. On July 24, 2008, FBI Agent Murray and an employee from Quality Alarm Service went to the Domicilio apartment complex to physically retrieve the defendant's historical electronic gate key access records from various gates.[29]

Second, the data was not retained by the alarm company, it was stored by Domicilio and the transactions were between the defendant and Domicilio.[30] Domicilio was not the target of the subpoena.

Third, other than to law enforcement, the uselessness of the geolocation data to Domicilio and Quality Alarm Service's business model is unsurprising considering it was kept in an inaccessible, crashed database of which a Domicilio employee had only recently learned about.[31]

11. *Manifest Factual Errors*: ***(a)*** Dkt. #1009, p. 39, ln. 10: "Defendant's computer and devices contained at least some encrypted information.";

Correction Supported By Evidence: What the Court does not understand is that all computers "contain[] at least some encrypted information." Nevertheless, the government decrypted the data of interest (*i.e.*, "filesalot.dcv") as soon as IRS-CI Agent Tracy L. Daun sat down at the defendant's computer.[32] By including the noted sentence in its order at Dkt.

---

29. *See Second Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 101.

30. *See id*.

31. *See id.*, EXHIBIT 099 and EXHIBIT 100 (Dkt. #821-6).

32. *See Fourth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 14 (Dkt. #898-1) (August 25, 2008 email from IRS-CI Agent Daun to AUSA Battista: "I was able to image each of the items and feel pretty confident that I have gotten around the encryption issue.").

#1009, the Court is seeding additional confusion to the effect that anyone reviewing the district court record may be led to believe that encrypted data played a role in the government's decision to conduct a 3+ year search of seized data storage devices. The Court's tactic, referred to as an "appellate cookie," was manifest error.

12. *Manifest Factual Errors*: ***(a)*** Dkt. #1009, p. 5, ln. 23-24: "Agents searched the suspect incident to his arrest and found a set of keys in his pocket.";

Correction Supported By Evidence: Federal agents neither arrested nor searched the defendant. The defendant was arrested and searched incident to arrest by an entity *separate from* the federal government, *i.e.*, the Santa Clara, CA police department.[33] The federal agents then later seized the keys from the actual arresting and searching entity.

13. *Manifest Factual Errors*: ***(a)*** Dkt. #1009, p. 5, ln. 25-26: "The agent waited for the arrival of other agents with the search warrant before entering the apartment.";

Correction Supported By Evidence: The agent who searched the keyhole was FBI Agent Vinh Nguyen[34] and he/she was not one of the agents who entered the apartment to search.[35]

II. Manifest Errors of Law

Various manifest errors of law are addressed in the subsections below. The defendant did not have time to address all manifest errors of law. Additionally, not all manifest errors of fact are referenced in the proceeding subsections. However, as a general matter, the defendant requests that the Court reevaluate ***all*** aspects of its legal analysis in light of the above facts that were corrected by the defendant for the Court.

---

33. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 06 (Dkt. #863-1) ("... Steven Brawner was arrested by **Santa Clara PD. Santa Clara PD conducted the search incident to arrest**. Vinh of FBI took possession of the keys that were in Brawner's pockets to check to see if they opened the apartment in question." (emphasis added)); *Second Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 106 (Dkt. #821-6) (same).

34. *See* fn. No. 33, *supra*.

35. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 06 (Dkt. #863-1) (list of the 10 federal agents who executed the search with **FBI Agent Vinh Nguyen not listed**).

A. The Court overlooked the defendant's argument that the N.D.Cal. 08-90330MISC order was not executed by the FBI technical agents who operated the equipment used to locate the aircard.

To recap the defendant's argument regarding non-execution: (1) there was no return filed with any court, (2) no one was ever served with the order, (3) the government is unable to produce evidence purportedly gathered under the order, (4) the government is unable to produce a single agent who can say he/she executed the order, and (5) the issuing magistrate permitted the government to arbitrarily edit the order's terms prior to execution and without judicial oversight. The mere existence of an order—which may have been edited by the government after it was issued—and a prosecutor's self-serving assertion that it was executed by unnamed agents is not sufficient to show that it was actually executed or that purported executing agents apprised themselves of the terms of the order. *See* Beier v. City of Lewiston, 354 F.3d 1058, 1069 (9th Cir. 2004) ("[T]he mere existence of a warrant provides little useful information to the officers."); United States v. Whitten, 706 F.2d 1000, 1009-10 (9th Cir. 1983) ("Officers conducting a search should read the warrant or otherwise become fully familiar with its contents..."). It was manifest error for the Court to ignore this argument.

1. The government's claim that non-technical agents witnessed the FBI technical agents operate the StingRay and KingFish lacks credibility.

During the March 28, 2013 hearing, AUSA Battista responded to the Court's question asking how the government might prove that the order was actually executed:

> [THE COURT:] ... Mr. Rigmaiden has argued that there is no evidence in this case that the warrant, Document 330, or Order 330, was used in the process of the mobile tracking device operation, was in the hands of the agents or was actually giving them guidance in the process. What is your response to that?
>
> MR. BATTISTA: Your Honor, obviously the government is not willing to disclose the identity of the technical agents, but **there are witnesses who have observed the technical agents doing their activities** and can hearsay the fact that they personally have spoken to the technical agents, and the technical agents were provided a copy of the order and reviewed the order....
>
> So the government, through -- if the Court needs it, the government is prepared through hearsay testimony to say that the agents had been spoken to, they were provided a copy of the warrant, they did review the warrant, **they**

> **were observed operating the equipment**,...
>
> *March 28, 2013 Motion Hearing Transcript*, p. 67-68 (emphasis added).

In other words, the government asserted that it would be willing to bring in the case agents to hearsay testify that they saw the FBI technical agents operate the StingRay and KingFish while the N.D.Cal. 08-90330MISC-RS order was in hand. AUSA Battista's claim made on March 28, 2013 directly contradicted his claim made in support of a different argument raised on September 22, 2011:

> [THE COURT:] Mr. Rigmaiden has been arguing that the government was using a StingRay produced by Harris. This document seems to support that.
>
> MR. BATTISTA: Let me respond to that, Your Honor.
>
> THE COURT: Yeah, please.
>
> …
>
> [MR. BATTISTA:] In the law enforcement world, there's a StingRay and then there's the generic term "StingRay" meaning all types of devices. The five case agents were using the term "StingRay" as the term "Kleenex." They did not operate the equipment. **They did not know what the equipment is**. They didn't receive any training on the equipment.
>
> ...None of the five investigators know the make, model, manufacturer of the exact equipment. There were tech agents out there. They're the ones who possessed the equipment, operated the equipment.
>
> ...They don't know. It could be a StingRay. It could not be. It could be something else. **They didn't know what it was. They didn't see it**...
>
> *September 22, 2011 Motion Hearing, Partial Transcript of Proceedings*, p. 35-36 (emphasis added).

The above discrepancy raises the classic lawyer question: "Were you lying then, or are you lying now?" Rather than continue to ignore it, the defendant requests that the Court address the defendant's argument regarding the government's failure to execute the N.D.Cal. 08-90330MISC-RS order. Especially in light of AUSA Battista's *post hoc* recharacterization of relevant facts designed to quell the Court's concerns raised on March 28, 2013. This is, in effect, new evidence considering the defendant only recently received the transcript for the March 28, 2013 hearing.

B. The Court overlooked the *independent* search/seizure concessions established at the January 27, 2012 status conference and ignored the defendant's scope arguments applying those concessions to the N.D.Cal. 08-90330MISC and 08-90331MISC-RS orders.

As the below quoted transcript shows, both the Court and the government agreed on January 27, 2012 that (1) the defendant would be permitted to identify and classify separate government actions into independent Fourth Amendment searches and seizures, and (2) the government would not later argue that each independent government action fails to meet the definition of a search and/or seizure—unless the defendant makes a silly argument such as classifying "the act of driving the vehicle[]" as a Fourth Amendment search:[36]

> [THE DEFENDANT:] But, I mean, even with the Government conceding that a search and seizure occurred, like I was saying earlier, I have to prove specific action[s] for searches and seizures. At least that's my interpretation of the cases I've read.
>
> So I can't just subtract that whole [factual] section out of my [suppression] motion just because they conceded that some type of search, some type of seizure occurred. They haven't actually identified what they searched or what they seized.
>
> ...
>
> THE COURT: ... Tell me in a nutshell what it is you're saying, because I agree, Mr. Rigmaiden needs to know --
>
> MR. BATTISTA: Sure.
>
> THE COURT: -- what he should have to address.
>
> MR. BATTISTA: Well, Your Honor, I think the position of the Government is that, you know, we are conceding in the abstract that what the Government did and the Court can assume is a search or seizure. But the defendant still has the burden of showing that he had an expectation of privacy in whatever was searched or seized....
>
> ...
>
> [THE COURT:] Well, so for purposes of what Mr. Rigmaiden is going to be writing, and to be very clear, the Government is conceding that the actions it took in the air card locating mission were sufficiently intrusive to constitute a Fourth Amendment search and seizure if the defendant had a reasonable expectation of privacy in the air card, in the laptop, in the apartment, in the signals that were sent out by the air card, et cetera?
>
> MR. BATTISTA: Correct, Your Honor.
>
> THE COURT: So it sounds like you do need to address reasonable expectation of privacy, Mr. Rigmaiden.
>
> ...

36. *January 27, 2012 Status Conference, Partial Transcript of Proceedings*, p. 25, *et seq*.

[THE COURT:] Mr. Rigmaiden doesn't have to prove [for example] that the Government wrote data to the air card in order to show that **the action** was sufficiently intrusive to constitute a Fourth Amendment search, because the Government is conceding the intrusiveness part of the Fourth Amendment analysis.

MR. BATTISTA: Correct, Your Honor.

THE COURT: Do you agree with that? Namely, you agree that you are conceding that -- well, it's what I've already said, that the air card locating mission was sufficiently intrusive to trigger Fourth Amendment protection if he has a reasonable expectation of privacy. Therefore, he doesn't have to prove the intrusiveness of any particular action in order to establish it was sufficiently intrusive for a Fourth Amendment violation.

MR. BATTISTA: That's correct.... So but that, I think the defendant's concern there is that goes more to possibly the Government having exceeded the scope of the order. I think that's what the defendant has said.

[THE COURT:] Do you have things you wanted to say on this, Mr. Rigmaiden?

THE DEFENDANT: Yes. Does that mean [][I] don't have to prove all of these individual, specific actions were searches and seizures? Like the Government is now conceding that if, as a factual matter, I can prove that they wrote data to the air card, then that was a Fourth Amendment search and seizure. And if as a factual matter I can prove that they deactivated encryption or read data from the air card, seized stored data on the air card, as long as I can prove all of that as a factual matter, then I don't have to actually prove that those are Fourth Amendment searches and seizures, because they are already admitting that they are. Is that what the Government --

THE COURT: The way I think I would say it, and see if this is right, Mr. Battista, is --

MR. BATTISTA: I'm listening, Your Honor.

THE COURT: Yeah, I want you to hear this. Let's take writing data to the air card as one example. Let's take increasing power consumption on the laptop as a second example. And let's take locating the air card precisely in the apartment as a third example.

It seems to me what the Government has conceded is that **any one of those three** is sufficiently intrusive to constitute a Fourth Amendment search if Mr. Rigmaiden had a reasonable expectation of privacy in the apartment and the laptop and the air card.

We are not going to come back if he, for example, asserts that this increased power consumption on the computer and argue, well, even if he had a reasonable expectation of privacy in the computer, even if you find that, Judge, increasing power isn't sufficiently intrusive to constitute a Fourth Amendment search. You are not going to make that argument because you are conceding intrusiveness. Is that correct?

MR. BATTISTA: Your Honor, I think that we would be willing to

> concede that it is part of the search. I mean, I think we may end up arguing with the defendant as to whether or not it's reasonable or not reasonable, whether or not it exceeded the scope of the warrant or whatever. But I think the -- obviously two and three that the Court mentioned, we would be conceding that it was -- that that was part of the air card mission -- that would possibly have been part of the air card mission. **And that we had conceded that all of the -- those aspects or similar aspects of the air card mission can be considered a search by the Court**.
>
> **...**
>
> THE COURT: Here's where I see it coming up. Let's say in his motion to suppress he has three pages where he argues that you had Verizon write data to the air card. Let's leave that one. Let's say he has three pages saying that you wrote data to the air card, your device did that, puts in all of his facts. It seems to me what **you cannot come back and argue** is, even if that's true, Judge, **writing data to an air card is not sufficiently intrusive to constitute a Fourth Amendment search**.
>
> MR. BATTISTA: I don't think we would do that, Your Honor...
>
> *January 27, 2012 Status Conference, Partial Transcript of Proceedings*, p. 13-23 (emphasis added).

Contrary to the discussion at the January 27, 2012 hearing, the government argued in its response brief (Dkt. #873) that the government actions identified/classified by the defendant into independent searches and/or seizures were not searches or seizures at all, but merely *Dalia*[37] style details of "how the Aircard is to be located or what actions will be taken to locate the Aircard." Dkt. #873, p. 51. Following the government's lead, the Court then ignored all of the defendant's scope arguments, adopted the government's application of *Dalia*, and denied the defendant's *Motion To Suppress* (Dkt. #824-1).

The Court dishonored the conditions and concessions upon which the suppression issues were to be decided. It was manifest error for the Court to disregard the defendant's scope challenges corresponding to what *should have been* uncontested, independent Fourth Amendment searches and seizures. Other Courts have also recognized the types of independent searches and seizures that were recognized by the Court and government on January 27, 2012:

> The "search" for which the Government seeks authorization is actually two-fold: (1) a search for the Target Computer itself, and (2) a search for digital information stored on (or generated by) that computer....
> Here... the installation of software which will "extract" (i.e. seize) the computer data... is itself a search or seizure that separately requires a warrant.

37. *See* Dalia v. United States, 441 U.S. 238 (1979).

In Re Warrant To Search A Target Computer At Premises Unknown, No. H-13-234M, Doc. #3, p.5 & 6, fn. 5 (S.D.Tex. Apr. 22, 2013).

1. In light of what was discussed on January 27, 2012, the Court overlooked scope and probable cause challenges relating to the 08-90331MISC-RS order.

Had the Court stuck to what was agreed upon, the following conceded, independent Fourth Amendment searches and seizures would have been accepted as fact for the purposes of ruling on all suppression issues relating to the operation of the SF-Martinez DCS-3000 Pen/Trap device:

Relating to SF-Martinez DCS-3000 Pen/Trap device

1. Verizon Wireless writing data to the aircard via OTAPA was a Fourth Amendment seizure. [Seizure that interferes with property/possessory interest in an "effect" (*Jacobsen* meaningful-interference-with-possessory-interest analysis)]. *See* Dkt. #824-1, p. 276.

2. Verizon Wireless reprogramming the aircard via OTAPA, or flashing its firmware over-the-air, was a Fourth Amendment seizure. [Seizure that interferes with property/possessory interest in an "effect" (*Jacobsen* meaningful-interference-with-possessory-interest analysis)]. *See* Dkt. #824-1, p. 277.

3. The FBI using the SF-Martinez DCS-3000 Pen/Trap device to obtain the defendant's real-time cell site sector location information relating to his use of the aircard was a Fourth Amendment search and seizure. [Trespassory search resulting in the obtaining of information (*Jones* trespass-to-obtain-information analysis) & Non-trespassory search that violates privacy resulting in the obtaining of information (*Katz* reasonable-expectation-of-privacy analysis)]. *See* Dkt. #824-1, p. 278.

4. The FBI using surreptitious phone calls to deny the defendant access to the Internet for six hours (*i.e.*, denial-of-service attack) was a Fourth Amendment seizure. [Seizure that interferes with property/possessory interest in an "effect" (*Jacobsen* meaningful-interference-with-possessory-interest analysis) & Seizure that interferes with an individual's liberty interest in a protected activity (*Soldal* meaningful-interference-with-

liberty-interest analysis)]. *See* Dkt. #824-1, p. 283.

* * *

The government relied upon the N.D.Cal. 08-90331MISC-RS order to justify the four conceded, independent searches and seizes listed above. As the defendant explained in his *Motion To Suppress*, the following places/items were searched by the government and/or Verizon during execution of the N.D.Cal. 08-90331MISC-RS order: **(1)** private residences, **(2)** the aircard, and **(3)** the host laptop computer used with the aircard.[38] Likewise, the following items/information were seized by the government and/or Verizon during execution of the N.D.Cal. 08-90331MISC-RS order: **(1)** the aircard, **(2)** the host laptop computer used with the aircard, **(3)** real-time cell site location information relating to the aircard while inside a private residence and not engaged in a call, **(4)** location of the aircard inside a private residence, and **(5)** the aircard Internet access service.[39] In its order a Dkt. #1009, the Court failed to address the defendant's scope and other challenges relating to the N.D.Cal. 08-90331MISC-RS order. This was manifest error. The N.D.Cal. 08-90331MISC-RS order does not list any of the above items/places corresponding to the conceded Fourth Amendment searches and/or seizures. Additionally, in the N.D.Cal. 08-90331MISC-RS order, there was absolutely no probable cause finding to support what the government has already conceded were independent Fourth Amendment searches and seizures.[40]

2. In light of what was discussed on January 27, 2012, the Court overlooked scope challenges relating to the 08-90330MISC-RS order.

Had the Court stuck to what was agreed upon, the following conceded, independent Fourth Amendment searches and seizures would have been accepted as fact for the purposes of ruling on all suppression issues relating to the operation of the FBI's cell site emulators (*i.e.*, the Harris brand StingRay and KingFish):

Relating to cell site emulators (*i.e.*, the Harris brand StingRay and KingFish)

38. *See* Dkt. #824-1, p. 326-328.
39. *See id*.
40. *See January 27, 2012 Status Conference, Partial Transcript of Proceedings*, p. 13-23.

1. The FBI forcing the aircard to handoff its 1xEV-DO Rel. 0 connection to the emulated cellular network broadcast by the StingRay and KingFish was a Fourth Amendment seizure. [Seizure that interferes with property/possessory interest in an "effect" (*Jacobsen* meaningful-interference-with-possessory-interest analysis) & Seizure that interferes with an individual's liberty interest in a protected activity (*Soldal* meaningful-interference-with-liberty-interest analysis)]. *See* Dkt. #824-1, p. 284.

2. The FBI repeatedly writing data to the aircard using the StingRay and KingFish was a Fourth Amendment seizure. [Seizure that interferes with property/possessory interest in an "effect" (*Jacobsen* meaningful-interference-with-possessory-interest analysis)]. *See* Dkt. #824-1, p. 286.

3. The FBI using the StingRay and KingFish to disable standard 1xEV-DO Rel. 0 air interface encryption for aircard signals was a Fourth Amendment seizure. [Seizure that interferes with property/possessory interest in an "effect" (*Jacobsen* meaningful-interference-with-possessory-interest analysis)]. *See* Dkt. #824-1, p. 287.

4. The FBI using the StingRay and KingFish to remotely access and download data from the aircard was a Fourth Amendment search and seizure. [Trespassory search resulting in the obtaining of information (*Jones* trespass-to-obtain-information analysis) & Non-trespassory search that violates privacy resulting in the obtaining of information (*Katz* reasonable-expectation-of-privacy analysis)]. *See* Dkt. #824-1, p. 288.

5. The FBI using the StingRay and KingFish to send location finding interrogation signals into the defendant's home and aircard was a Fourth Amendment search and seizure. [Trespassory search resulting in the obtaining of information (*Jones* trespass-to-obtain-information analysis) & Non-trespassory search that violates privacy resulting in the obtaining of information (*Katz* reasonable-expectation-of-privacy analysis)]. *See* Dkt. #824-1, p. 290.

6. The FBI using the StingRay and KingFish to collect the aircard's signal transmissions sent in response to the location finding interrogation signals was a Fourth Amendment search and seizure. [Trespassory search resulting in the obtaining of

information (*Jones* trespass-to-obtain-information analysis) & Non-trespassory search that violates privacy resulting in the obtaining of information (*Katz* reasonable-expectation-of-privacy analysis)]. *See* Dkt. #824-1, p. 291.

7. The FBI using the StingRay and KingFish to conduct triangulation techniques on aircard signals transmitted in response to interrogation was a Fourth Amendment search and seizure. [Non-trespassory search that violates privacy resulting in the obtaining of information (*Katz* reasonable-expectation-of-privacy analysis)]. *See* Dkt. #824-1, p. 293.

8. The FBI using the StingRay and KingFish to deny the defendant access to the Internet for ten hours (*i.e.*, denial-of-service attack) was a Fourth Amendment seizure. [Seizure that interferes with property/possessory interest in an "effect" (*Jacobsen* meaningful-interference-with-possessory-interest analysis) & Seizure that interferes with an individual's liberty interest in a protected activity (*Soldal* meaningful-interference-with-liberty-interest analysis)]. *See* Dkt. #824-1, p. 294.

9. The FBI using the defendant's electricity provided to his aircard and forcing the aircard to transmit at the highest possible power was a Fourth Amendment seizure. [Seizure that interferes with property/possessory interest in an "effect" (*Jacobsen* meaningful-interference-with-possessory-interest analysis)]. *See* Dkt. #824-1, p. 296.

* * *

The government claimed[41] that it was relying upon the N.D.Cal. 08-90330MISC-RS order to justify the nine conceded, independent searches and seizes listed above. As the defendant explained in his *Motion To Suppress*, the following places/items were *searched* by the government during its asserted execution of the N.D.Cal. 08-90330MISC-RS order: **(1)** private residences and other private areas, **(2)** the aircard, and **(3)** the host laptop computer used with the aircard.[42] Likewise, the following items/information were *seized* by the government during its asserted execution of the N.D.Cal. 08-90330MISC-RS order: **(1)** the

41. As previous noted in Section II(A), *supra*, the government failed to produce evidence showing that the N.D.Cal. 08-90330MISC-RS order was being executed during operation of the StingRay and KingFish.

42. *See* Dkt. #824-1, p. 303-306.

aircard, **(2)** the host laptop computer paired with the aircard, **(3)** ESN data stored on the aircard's internal storage device, **(4)** location finding response signals transmitted by the aircard, **(5)** geolocation data showing the location of the aircard, **(6)** aircard Internet access service, and **(7)** the electricity provided to the aircard and laptop by its user.[43]

In its order at Dkt. #1009, the Court only addressed the defendant's scope challenges relating to the "location search" conducted by the FBI using the StingRay and KingFish. From the nine independent searches and seizures listed above, the Court only arguably addressed ¶ No. 5 (interrogation signals) ¶ No. 7 (triangulation techniques) when rejecting the defendant's scope arguments relating to the "location search":[44]

> The Tracking Warrant precisely identified the object to be **located**, found probable cause to believe that **location** of the aircard would produce evidence of the crimes identified in the warrant and the identification of individuals involved in those crimes, and placed a time limit on the **location** effort. As noted above, the warrant also specifically recognized that the aircard may be **located** in a private residence.
>
> Dkt. #1009, p. 34 (emphasis added).

However, the Court failed to address the remainder of the defendant's scope challenges relating to the rest of the **independent** searches and seizures conceded by the government. During the January 27, 2012 status conference, the Court clearly distinguished the "location search" from the other independent searches and seizures applicable to the defendant's scope challenges:

> THE COURT: Yeah, I want you to hear this. Let's take writing data to the air card as one example. Let's take increasing power consumption on the laptop as a second example. And let's take locating the air card precisely in the apartment as a third example.
>
> It seems to me what the Government has conceded is that **any one of those three** is sufficiently intrusive to constitute a Fourth Amendment search...

---

43. *See id*.

44. The Court also failed to address, in the context of the "location search," the issue of the N.D.Cal. 08-90330MISC-RS order not listing the host laptop computer along with the aircard. Agents were aware at the time that the aircard was a PCMCIA card requiring a laptop computer to function. This is an additional scope violation not considered by the Court while it analyzed the "location search." Furthermore, the Court did not address the seizure of the aircard's transmitted signals, which is also an item not listed in the order.

> *January 27, 2012 Status Conference, Partial Transcript of Proceedings*, p. 13-23, *et seq.* (emphasis added).

Therefore, it was manifest error for the Court to apply *Dalia* as a means to ignore the rest of the defendant's scope challenges. An application of *Dalia* should only apply to actions such as "the act of driving the vehicle[]"[45] as was discussed on January 27, 2012.

Dalia clearly does not apply considering, for one thing, the government conceded to the independent Fourth Amendment activity of using the StingRay and KingFish to intrude into the defendant's aircard for the purpose of downloading the defendant's stored data.[46] This was a **search** of the aircard itself for the purpose of **seizing** stored data within the aircard. The N.D.Cal. 08-90330MISC-RS order does not authorize the government to **search** the aircard and it does not list the aircard's stored data as an item to be **seized**. Another example, the government conceded to using the defendant's electricity[47] and to denying the defendant access to the Internet.[48] This was a **seizure** of electricity and a **seizure** of aircard Internet access service. The N.D.Cal. 08-90330MISC-RS order does not authorize the government to **seize** the defendant's electricity and aircard Internet access service. The same reasoning applies to **seizing** location finding response signals transmitted by the aircard, geolocation information, the host laptop computer, *etc*. *See* Dkt. #824, p. 302-345.

Additionally, there was no probable cause findings[49] to support what the government has already conceded were independent Fourth Amendment searches and seizures. The probable cause finding in the N.D.Cal. 08-90330MISC-RS order only applied to the use and monitoring of a mobile tracking device—the order did not state that there was probable cause to search and seize anything at all. *See* Dkt. #1009, p. 23-24.

---

45. *January 27, 2012 Status Conference, Partial Transcript of Proceedings*, p. 25, *et seq*.
46. *See* Dkt. #824-1, p. 288.
47. *See* Dkt. #824-1, p. 296.
48. *See* Dkt. #824-1, p. 294.
49. Finding that there is probable cause to use and monitor a mobile tracking device does not apply to all of the other Fourth Amendment searches and seizures conceded by the government and ignored by the Court.

C. Even if the N.D.Cal. 09-90330MISC-RS order authorized use of a cell site emulator with the phrase "mobile tracking device," it was manifest error for the Court to not suppress evidence obtained using the *second*, handheld "mobile tracking device" within the Domicilio apartment complex.

The defendant has shown, without contradiction from the government, that the FBI technical agents used **two** separate cell site emulators (*i.e.*, devices the Court and government call "mobile tracking devices").[50] In his *Motion To Suppress*, Dkt. #824-1, Section V(F)(1), the defendant argued that the N.D.Cal. 08-90330MISC-RS order did not authorize the government to use the vehicle-transportable (*i.e.*, StingRay) and man-portable (*i.e.*, KingFish) cell cite emulators to locate the aircard. The Court disagreed. *See* Dkt. #1009. However, even if the phrase "use and monitor a mobile tracking device" applied to cell site emulators, the N.D.Cal. 08-90330MISC-RS order only authorized use of **one** "mobile tracking device," not **two**. Any evidence gathered by the second "mobile tracking device" is beyond the scope of the order and must be suppressed. *See* United States v. Juichang Chen, 979 F.2d 714, 719 (9th Cir. 1992) (Because evidence was gathered using an unauthorized third camera, "[t]he government has agreed to suppress all of the fruits of camera 3, and, under the facts of this case, this is a sufficient remedy."). It was manifest error for the Court to not suppress all evidence obtained by the **second** "mobile tracking device" used by the FBI, *i.e.*, the handheld cell site emulator used by agents while within the Domicilio apartment complex.

D. The Court misunderstood the defendant's argument regarding the operative section of the N.D.Cal. 08-90330MISC order failing to command or authorize use of a mobile tracking device, notwithstanding the probable cause finding.

The Court misconstrued the defendant's scope argument as claiming: "Judge Seeborg's probable cause finding applied only to information provided by Verizon and not to locating the aircard." Dkt. #1009, p. 24. The defendant did not make this argument. The defendant argued that the operative section of the order, that which commands the search, did not command or authorize **anyone** (*i.e.*, the government or Verizon Wireless) to use a "mobile

50. *See* Dkt. #824-1, p. 162, ¶ No. 10.

tracking device." *See* Dkt. 824-1, p. 309, Section V(F)(1)(b). The N.D.Cal 08-90330MISC-RS order suffers the same fatal flaw suffered by the warrant discussed in United States v. Robinson, 358 F. Supp. 2d 975 (D.Mont. 2005). In *Robinson*, law enforcement relied upon a warrant to search a residence while "the operative portion of the warrant, that which commands the search, d[id] not include a reference to the residence..." *Id.* at 977. The *Robinson* court found that a warrant is invalid if it "omits the residence from the command section[]" even if the warrant contains "an explicit finding of probable cause to search the residence." *Id.* at 979.[51] In the present case, the operative section of the order does not command or authorize use of a "mobile tracking device." It was manifest error for the Court to overlook this controlling issue.

E. In light of the Ninth Circuit's *Oliva* opinion, the Court erroneously applied *Dalia* to the separate issue of the government failing to describe its surveillance technology in the N.D.Cal. 08-90330MISC-RS order.

First, the Court was apparently misled by the government's response to the defendant's *Motion To Suppress* which incorrectly asserted that "defendant argues that the execution exceeded the scope because the warrant did not specifically authorize the FBI to use a cell site simulator..."[52] Using its straw man, the government argued that *Dalia* allows the government to omit crucial details in orders when using new technology to conduct Fourth Amendment searches and seizures.[53] In reply to the government's *Dalia* argument, the defendant pointed out to the Court that he did **not** argue at Dkt. #824-1 that the government's failure to explain the technology was a Fourth Amendment violation.[54] In fact, in the hundreds of pages identifying and classifying the numerous independent Fourth Amendment

---

51. The Robinson Court rejected the government's "cut and paste" error argument and found that "[t]he Fourth Amendment's warrant requirement has no exception for a mistake in cutting and pasting, nor does it authorize a reviewing court to divine what seems obvious but is clearly outside the scope of the application and warrant authorizing the search." *Id.* at 976.

52. Dkt. #873, p. 50-51.

53. *Id*.

54. *See* Dkt. #900, p. 25-27.

searches and seizures that were conceded by the government,[55] the defendant did not once attempt to distinguish *Dalia* on the grounds that the StingRay/KingFish technology was not explained.[56] As the defendant already explained, *Dalia* is entirely irrelevant to how the parties agreed the suppression issues would be decided. *See* Section II(B), *supra*. However, in dealing with the government's application of *Dalia* at Dkt. #900, the defendant asserted that it is still a Fourth Amendment violation when the government fails to explain new surveillance technology. The defendant argued that new surveillance technology should be explained so that issuing magistrates will have the "opportunity to understand all the resulting necessary Fourth Amendment implications prior to deciding whether to issue the order as drafted by the government."[57] The defendant presented this argument for the first time in his reply considering the government raised the issue for the fist time in its response. Thereafter, the ACLU and EFF filed an *Amici* brief in large part supporting the defendant's counter to the government's attempt to apply *Dalia*. Apparently, this series of events caused the Court to experience confusion over what was discussed at the January 27, 2012 status conference. *See* Section II(B), *supra*. Determining the Court's confusion before it was even revealed, the defendant went to great efforts during the March 28, 2013 motions hearing to explain the independent Fourth Amendment searches/seizures while stressing that "[t]his issue is **completely separate** from the [] order not explaining the technology at issue, which is a separate Fourth Amendment violation altogether."[58]

In light of this motion for reconsideration, the defendant hopes that the Court will now honor what was discussed and agreed upon on January 27, 2012. However, if the Court still insists on dishonoring the concessions established at the January 27, 2012 status conference, it is still manifest error for the Court to ignore the controlling Ninth Circuit case law

---

55. *See* Dkt. #824-1.

56. In a separate section, the defendant argued that the government cannot claim good faith for scope violations considering it did not put forth effort to describe the technology to the issuing magistrate, which would have allowed him to decide whether additional independent searches and seizures required authorization in the order. *See* Dkt. #824-1, p. 354-355.

57. Dkt. #900, p. 28.

58. *March 28, 2013 Motion Hearing Transcript*, p. 24 (emphasis added).

effectively distinguishing *Dalia* from searches and seizures involving new surveillance technology:

> We agree that if the government seeks authorization for the use of **new technology**..., it must specifically request that authority, the court must scrutinize the need for such surveillance and the authorization orders must be **clear and unambiguous**.
>
> United States v. Oliva, No. 10-30126, p. 8371 (9th Cir., Jul. 20, 2012) (emphasis added);
>
> *See also* In Re Warrant To Search A Target Computer At Premises Unknown, No. H-13-234M, Doc. #3, p. 8 (S.D.Tex. Apr. 22, 2013) (Rejecting warrant application for use of new technology because "[t]he Government's application contains little to no explanation of how the Target Computer will be found.").

F. It was manifest error for the Court to consider the N.D.Cal. 08-90330MISC-RS order application and affidavit while it was not incorporated by reference or present during use of the StingRay and KingFish.

The Court's findings relating to particularity and scope absolutely depended on an erroneous consideration of the N.D.Cal. 08-90330MISC-RS order application and affidavit:

> The Court concludes, however, that "mobile tracking device" is a reasonable description of the mobile device used by the government to track the aircard. The Tracking Warrant authorized "the use and monitoring of a mobile tracking device for the Target Broadband Access Card/Cellular Telephone," while "the agents are stationed in a public location and the Target Broadband Access Card/Cellular Telephone is . . . inside private residences, garages, and/or other locations not open to the public or visual surveillance[.]" Id. at 28-29. **The affidavit of Agent Ng stated that the mobile tracking device would monitor the aircard and would "ultimately generate a signal that fixes the geographic position of the [aircard]."** *Id.* at 26.
>
> Dkt. #1009, p. 24-25 (emphasis added).

The Court considered the underlying application and affidavit even while there is no evidence of those documents (or even the order itself) being present during operation of the StingRay and KingFish:[59]

> THE COURT: Well, I understand you're arguing that the order is sufficiently particular. I just wanted to make sure you agreed that as I do that analysis, I need to look at the face of the order and not the affidavit, because we don't know if it was in the possession of the executing agents. It sounds like you agree with that.
>
> *March 28, 2013 Motion Hearing Transcript*, p. 70.

59. *See* Section II(A), supra.

Despite the above, the Court relied upon United States v. Smith, 424 F.3d 992 (9th Cir. 1992) to find in its order that "Defendant apparently 'confuses the well-settled principle that a warrant's overbreadth can be cured by an accompanying affidavit that more particularly describes the items to be seized with the contention... that an affidavit incorporated by reference must always be attached for the search warrant to be valid – even if the warrant is not overbroad without the attachment.'" Dkt. #1009, p. 33 (citation omitted). It is the Court who is confused, not the defendant. The Ninth Circuit made clear in *Smith* that "failure to attach the affidavit d[id] not require suppression[]" because "the warrant without the affidavit was facially valid standing alone." *Id.* at 1007-1008. Clearly, if the N.D.Cal. 08-90330MISC-RS order "was facially valid standing alone," the Court would have had no need to rely upon the underlying application and affidavit as it did in its order.[60] It was manifest error for the Court to consider the unincorporated/unaccompanied underlying application and affidavit in light of United States v. SDI Future Health, Inc., 553 F.3d 1246, 1258 (9th Cir. 2009) and similar cases.

G. The Court made numerous manifest errors of law relating to the government's digital data search.

1. It was manifest error for the Court to overlook the defendant's *temporal scope* argument relating to digital data.

The N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants used by the government to search and seize digital data from the seized computer system state that the government may only expose and search for files "[f]or the period January 1, 2005, through the present[.]"[61] In a prior filing[62] and during oral arguments, the defendant pointed out that **70.88%** of the files on the seized "T" drive were dated prior to that time period.[63]

---

60. While the Court cited the underlying documents after a heading labeled "Probable Cause," the defendant never challenged the underlying probable cause statement and the quoted section of the Court's order was clearly a scope analysis acting as the foundation for all other findings relating to scope and particularity.

61. *E.g.*, *Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No. 1122*, *Warrant* (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #566-2, p. 5).

62. The defendant had to submit his own technical declarations considering the Court denied the defendant's motion for appointment of an expert.

63. *See March 28, 2013 Motion Hearing Transcript*, p. 15-16 ("The warrant also

Evidence of this fact is on the record at Dkt. #962-1. In other words, the number of files on the "T" drive dated prior to January 1, 2005 is a whopping **37,941** out of **53,521** files.[64] With that in mind, the Court found that "the government [] conduct[ed] a thorough, **file-by-file review** of the items seized pursuant to the search warrant." Dkt. #1009, p. 41 (emphasis added). Additionally, the defendant proved that government personnel opened and read using "human eyes" and/or software **53,342** files out of a total of **53,521** files (**99.66%** of all files) on the defendant's "T" drive (*i.e.*, "filesalot.dcv"),[65] which is the drive containing the bulk of the seized evidence in this case. Therefore, the government illegally viewed the **37,941** files on the "T" drive that were beyond the temporal scope of the warrant.

The defendant also proved that the software used by IRS-CI Agent Daun during her forensic examination had features allowing for compliance with temporal scope limits contained in warrants.[66] Therefore, "right off the bat, the government could have very easily only exposed [the] 29.12 percent of files [on the 'T' drive] which would have been after January 1st, 2005, as opposed to exposing 99.66 percent of the files."[67] This argument also applies to all other drives considering, as the Court noted, the government conducted a thorough, file-by-file review of all seized drives. By viewing all files, *e.g.*, even those files too old to be covered by the warrant, the government conducted an impermissible general search. In denying one of the defendant's arguments, the Court noted that "the SCA Order that authorized disclosure of the IP addresses was limited as to time, seeking only those addresses accessed by the aircard between March 1 and July 9, 2008." Dkt. #1009, p. 20. What a double standard. It was manifest error for the Court to not consider the temporal

---

prohibited the government from seizing any file from a period prior to January 1st, 2005. Between 62.65 percent and 73.97 percent of all files on any given seized drive were dated prior to that time period. And I explained this in my technical declarations on the record at 962-1, 963-1, 964-1, and 965-1. For the T drive specifically, which is a drive the government seized the bulk of the evidence, 70.88 percent of all files were beyond just the temporal scope of the warrant."). Note: the defendant made these arguments as soon as his technical analysis was complete. Again, the Court refused appointment of an expert.

64. *See* Dkt. 962-1.

65. *See* Dkt. 961-1.

66. *See March 28, 2013 Motion Hearing Transcript*, p. 16.

67. *See id*.

scope violations conducted by the government when searching digital data under the N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants.

2. It was manifest error for the Court to overlook the core of the defendant's minimization argument relating to digital data.

The N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants expressly required that government agents employ means designed to "locate and expose only those categories of files, documents, or other electronically stored information that are identified with particularity in the warrant..."[68] The Court found as follows regarding the government's failure to comply with the express minimization requirements:

> Defendant argues in a supplemental filing that Agent Daun violated the protocol's requirement that she minimize the examination of out-of-scope materials while searching the copies of Defendant's computer and storage devices because she looked at files herself rather than conducting a key-word search for relevant files. Doc. 934-1 at 13-14. The Court is not persuaded that Agent Daun's method of viewing the files constitutes a violation of the protocol. Even the best key-word searches miss relevant information, and the Court cannot fault the government for conducting a thorough, file-by-file review of the items seized pursuant to the search warrant. *See United States v. Giberson*, 527 F.3d 882, 889 (9th Cir. 2008) (rejecting argument that government was required to rely on folder names or other limited means of searching computer files, noting that such searches may miss critical evidence hidden as part of criminal activity).
>
> Dkt. #1009, p. 41, fn. No. 10.

However, the defendant provided "keyword searches" as one of many options the government could have pursued in order to comply with the warrants' minimization terms. The defendant did not argue that the government was required to conduct keyword searches. The defendant's argument was clear:

> [T]the defendant need not posit any effective alternative search method considering file-by-file, "human eye" review is the epitome of doing absolutely **nothing** in terms of limiting agent exposure to *out-of-scope* data." Although no specific guidelines were provided, the relevant warrants required that the government do *something* and by doing *nothing* the government clearly violated the warrants' minimization terms.
>
> Dkt. #934-1, p. 26.

---

68. *E.g.*, *Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No.* 1122, *Warrant*, "Computer Search Protocol For The Northern District Of California" (Dkt. #566-2, p. 17).

In any event, the Court erred when it relied upon United States v. Giberson, 527 F.3d 882, 889 (9th Cir. 2008) to reject the defendant's argument. The search warrant in *Giberson*, as well as the search warrants addressed in all other Ninth Circuit cases, do **not** contain the express minimization terms incorporated into the warrants in the present case. Furthermore, the Ninth Circuit previously made clear that "it is important to preserve the option of imposing [][search] conditions when they are deemed warranted by judicial officers authorizing the search of computers." United States v. Payton, 573 F.3d 859, 864 (9th Cir. 2008). The purpose of these conditions, like the conditions relevant here, are "to protect privacy and other important constitutional interests." *Id*. By doing **absolutely nothing** to comply with the minimization terms incorporated into the warrants by the issuing magistrates, the government exceeded the scope of the warrants. The government failed to even comply with the temporal scope limits and needlessly exposed **37,941** *out-of-scope* files on just one hard drive. *See* Section II(F)(1), *supra*. This minimization violation alone shows a fishing expedition.

With concerns of how computer searches are conducted in the Northern District of California, the Court's own reasoning dictates following District Judge Ronald M. Whyte, with his finding that using software and word searches is a good way to comply with the minimization requirements contained in the "Computer Search Protocol For The Northern District Of California":

> "By using software and word searches, the government avoided looking at documents that were likely to be outside the scope of the warrants." With this method, "only those documents that had a likelihood of being within the scope of the warrant were examined by human eyes. Thus, potential Fourth Amendment concerns were minimized."
>
> United States v. Fu-Tain Lu, 2010 U.S. Dist. LEXIS 144395, CR-09-00341 RMW (N.D.Cal., Sept. 16, 2010).

It was manifest error for the Court to overlook the government's failure to do anything at all to comply with the minimization terms contained in the N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants.

3. It was manifest error for the Court to find that the government acted in good faith while relying upon incorrect advice from the N.D.Cal. U.S. Attorneys office.

The Court found that the government acted in good faith while following the incorrect advice provided by the N.D.Cal. U.S. Attorneys office:

> [T]he government did not deliberately violate the protocol. It sought the advice of the Northern District of California concerning interpretation of the protocol, and the interpretation was not clearly unreasonable. *CF. United States v. Koch*, 625 F.3d 470, 478 (8th Cir. 2010).
>
> Dkt. #1009, p. 45.

The Court relied upon an Eighth Circuit case to make the above finding. In doing so, the Court ignored binding Ninth Circuit precedent:

> We reject the conclusion of the district court that the officers are insulated by qualified immunity because of their reliance on the approval given by an attorney and the magistrate who signed the warrant.... [T]he fact that a warrant was reviewed by two Assistant United States Attorneys and signed by a magistrate does not amount to 'exceptional circumstances' on the basis of which a reasonable officer could rely... The officers applying for the warrants in this case did not ask for, nor did they receive any such specific assurances from the magistrate issuing the warrant.
>
> Marks v. Clarke, 102 F.3d 1012, 1028 (9th Cir. 1996).

In light of *Marks*, it was manifest error for the Court to find that the government acted in good faith based on its own self-serving assurances – *if* those assurances even occurred. Additionally, the warrants at issue expressly state that "[t]he government must promptly notify the judge who authorized issuance of the search warrant (or, if that judge is unavailable, to the general duty judge) if a dispute arises about rights or interests in any seized or searched item..."[69]

4. It was manifest error for the Court to find the 30-day search window violations were (1) not unattenuated but-for causes of obtaining digital evidence, and (2) justified by exigent circumstances.

The court found that the 30-day search window violations, which were also scope

69. *E.g.*, *Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No.* 1122, *Warrant*, "Computer Search Protocol For The Northern District Of California" (Dkt. #566-2, p. 17).

violations, were not a but-for cause of obtaining digital evidence:

> The government erred in not seeking an extension of the warrant to permit continued searching of the computer and storage device copies. If the government had not made this error – if it had obtained the extension – all of the evidence on the laptop and storage devices would have been found under the Amended Warrant.
>
> Dkt. #1009, p. 45.
>
> [T] he Supreme Court has held that violation of a magistrate judge's directives in executing a search warrant does not necessarily require suppression. In *Richards v. Wisconsin*, 520 U.S. 385 (1997), the magistrate who executed the search warrant specifically deleted the portion of the warrant that authorized officers to make a no-knock entry. When the search warrant was executed, however, officers concluded that the defendant was about to dispose of drugs and made a no-knock entry. The defendant argued before the Supreme Court that this action directly violated the magistrate's warrant and required suppression. The Supreme Court disagreed, holding that the officers' actions were reasonable in light of the circumstances they encountered when they arrived at the scene. *Id.* at 396-97.
>
> Dkt. #1009, p. 44.
>
> The Court misunderstands unattenuated but-for causation as discussed in *Hudson*.[70]

Additionally, the Court misunderstands exigent circumstances as discussed in *Richards*. First, if analyzed in the context of a *Hudson* no-knock style technical violation, the search was unreasonable, the seized data would not have come to light but-for the 30-day search window violations, no attenuation can be realized, and suppression is merited. The government had two options under the warrants after expiration of the 30-day deadlines: (1) stop searching for data, or (2) obtain an extension of time to continue the search. Because the challenged violations involve **the government's failure to stop searching after 30 days**, determining but-for causality is done by examining the search as if the government had, in fact, **stopped searching**. Under this examination, no evidence would have been obtained by the government after the first 30 days and, as a result, the necessary but-for causality is satisfied. The government's failure to obtain an extension of time is a separate violation that occurred after the government violated the terms to stop searching after 30-days. It was manifest error for the Court to skip over the challenged violation and venture into hypothetical land—especially when the government had absolutely no plans to obtain an

70. Hudson v. Michigan, 547 U.S. 586, 592 (2006)

extension of time and never informed the issuing magistrates that agents violated the terms of the warrants.

Having established but-for causality under *Hudson* for the 30-day search window violations, attenuation is determined[71] by examining the two factors discussed in *Hudson*: (1) evidence relation to violation, and (2) suppression remedy relation to purpose.[72] Under this examination, there is no attenuation of the evidence considering (1) the causal connection between the evidence and violation is not too remote,[73] and (2) suppression of the evidence bears a relation to the purposes of which the 30-day search windows were to serve, *i.e.*, limiting lengthy human-eye exposure to private data.[74] Therefore, suppression is merited under *Hudson*.

Second, in an attempt to sidestep *Hudson*, the government justifies its 30-day search window violations by relying on Richards v. Wisconsin, 520 U.S. 385, 395-96 (1997), a pre-*Hudson* knock-and-announce violation case. In *Richards*, the Supreme Court said that "the reasonableness of the officers' decision[] [to commit a technical violation] must be evaluated as of the time [the violation occurred]." *Id*. The *Richards* decision was based on the reasoning that a magistrate cannot "anticipate[] in every particular the circumstances that would confront the officers when they [conduct a search]." *Id*. In other words, in order to justify a technical violation, the government must show how exigent circumstances prevented it from first seeking authorization from a magistrate. For example, in pre-*Hudson* United States v. Granville, 222 F.3d 1214 (9th Cir. 2000), the Ninth Circuit suppressed

---

71. "Our cases show that but-for causality is only a necessary, not a sufficient, condition for suppression." Hudson, 547 U.S. at 592.

72. "Attenuation can occur, of course, when the causal connection is remote. Attenuation also occurs when, even given a direct causal connection, the interest protected by the constitutional guarantee that has been violated would not be served by suppression of the evidence obtained." *Id.* at 593 (internal citation omitted).

73. Just like in *Thompson*, because the violations "were all executed in the course of enabling the executing agents to conduct their search and seizure..., the unreasonableness cannot be separated from the search and subsequent seizure." United States v. Thompson, 667 F. Supp. 2d 758, 767 (S.D. Ohio 2009).

74. *Compare* United States v. Ankey, 502 F.3d 829, 836 (9th Cir. 2007) ("The Supreme Court made it clear that, because the knock-and-announce rule protects interests that 'have nothing to do with the seizure of... evidence, the exclusionary rule is inapplicable' to knock-and-announce violations." (*quoting* Hudson, 547 U.S. at 594)).

evidence for a knock-and-announce violation considering law enforcement's "failure to comply was not justified by exigent circumstances." *Id.* at 1220 (applying *Richards*). In the present case, the government has identified no exigent circumstances justifying its 30-day search window violations or its failure to request extensions of time from a magistrate over the course of a 3+ year long unauthorized search period.

Turning back to *Hudson*, the government's mere unexercised option to seek an extension of time does not act to attenuate the evidence from the noted violations or eliminate but-for causality. For example, had the court in *Hudson* found that the knock-and-announce violation ***was*** an unattenuated but-for cause of obtaining the evidence, the government would have been hard pressed to claim that the evidence was admissible simply because agents *could have* gone back to the magistrate at any time—either before or after the violation—to have the no-knock authority added to the warrant's terms. In the present case, one can only speculate as to whether the government *would have* applied for an extension of time in some hypothetical parallel universe, or whether the extension *would have* been for an additional week, an additional 3+ years, or even been granted at all. Furthermore, one can only speculate as to whether the issuing magistrate *would have* imposed additional restrictions when issuing the extension or whether the government *would have* complied with those restrictions or engaged in additional Fourth Amendment violations. In sum, once the necessary but-for causality is established, the government's mere unexercised option to properly conduct a search is not an avenue to attenuation. There is absolutely no support in case law for the Court's reasoning.

Furthermore, the government having the evidence in its possession is not a means to obtain now what was illegally obtained then, or a means to show attenuation vis-a-vis the original violations. For example, if unattenuated but-for causality had been found in *Hudson*, the government would have been hard pressed to claim that the finding was extraneous simply because the evidence was already in the government's possession (*e.g.*, in a government storage locker), which could then be searched and seized using a new warrant. Furthermore, the warrants at issue in the present case required destruction of all *out-of-scope*

data after 60 days. Had the government complied with those terms, there would have been no evidence to search after 60 days—let alone 3+ years. It was manifest error for the Court to not suppress evidence in this context.

5. It was manifest error for the Court to find no Fourth Amendment violation in light of IRS-CI Agent Daun waiting six months to start here forensic examination while all other agents searched clones of the defendant's computer.

The Court found acceptable IRS-CI Agent Daun taking six months to even begin here forensic examination (*i.e.*, the process meant to determine whether any irrelevant, personal information was improperly seized):

> Defendant argues that Agent Daun waited six months to be[g]in[] her "forensic analysis" of relevant files, but notes that she and others were reviewing information on copies of the computer and storage devices during this six-month period. Doc. 934-1 at 5–6. In *Metter*, by contrast, the government conducted no review of seized materials for a period of 15 months after the search warrant was executed.
>
> Dkt. #1009, p. 46, fn. No. 11.
>
> Nor can the Court conclude that the government unreasonably delayed its search of the device copies. Searches were started immediately, and extended over the ensuing months given the volume of the information to be reviewed. *See United States v. Metter*, 860 F.Supp.2d 205, 211-16 (E.D.N.Y. 2012) (finding suppression the appropriate remedy where the government retained copies of seized computer hard drives for more than 15 months without any review to determine whether the imaged electronic documents fell within scope of search warrants).
>
> Dkt. #1009, p. 45.

First, unlike the warrants at issue in the present case, the warrant in *Metter* contained no express time limits designed to limit exposure to *out-of-scope* data. The Ninth Circuit follows the reasoning that "judges issuing warrants may place conditions on the manner and extent of such searches, to protect privacy and other important constitutional interests." Payton, 573 F.3d at 864. Second, it was further manifest error for the Court to disregard the six month delay in isolating *in-scope* data from *out-of-scope* data merely because "[s]earches were started immediately[.]" Dkt. #1009, p. 45. The immediate searches noted by the Court were conducted in further violation of the warrants terms and the defendant's Fourth Amendment rights. During the six month period of which IRS-CI Agent Daun failed to even

begin her forensic analysis, three additional untrained case agents were accessing their own personal clones of the defendant's entire computer system with no mechanism in place to shield them from *out-of-scope* data. Therefore, the six month delay in the present case was far more intrusive than the stagnant fifteen month delay found unconstitutional in *Metter*. Third, it was further manifest error for the Court to justify the delay "given the volume of the information to be reviewed." Dkt. #1009, p. 45. IRS-CI Agent Daun candidly admitted that she could have been finished with the entire forensic examination in roughly **60 days**, *i.e.*, "by late March or early April [of 2009]."[75][76] Note: IRS-CI Agent Daun began her forensic examination on February 2, 2009. Furthermore, the defendant explained during oral arguments that the forensic software IRS-CI Agent Daun had available "let's you run in a single automated session a collection of powerful analytic tools. Since you can run the evidence processor unattended, you can work on other aspects of the case while this tool is processing data."[77] Under the circumstances of this case, it was manifest error for the Court to find that it was reasonable for the government to take six month to even "*begin* review of [][seized] data to determine whether any irrelevant, personal information was improperly seized."[78]—while numerous agents arbitrarily accessed clones of the defendant's entire computer without any mechanism in place to shield their eyes from *out-of-scope* data.

---

75. *See Sixth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #933-1).

76. Furthermore, the October 22, 2012 prosecution report indicates that IRS-CI Agent Daun took one to three calendar days to examine most of the forensic images. *See Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #929-1, p. 8-9).

77. *March 28, 2013 Motion Hearing Transcript*, p. 13 (emphasis added).

78. United States v. Metter, No. 10-CR-600 (DLI), Doc. 219, p. 16 (E.D.N.Y., May 17, 2011) ("The government's blatant disregard for its responsibility in this case is unacceptable and unreasonable."). Notably, the *Metter* court found a Fourth Amendment violation even while the applicable warrant had no express time limitation like the warrants relevant in the present case.

H. The Court made numerous manifest errors of law while determining whether the defendant had a reasonable expectation of privacy in his home residence, aircard, laptop computer, *etc.*

1. Application of corrected facts vis-a-vis manifest factual errors.

The Court found that the defendant had no reasonable expectation of privacy in his home residence and possessions because:

> Defendant rented the apartment using the name of a deceased individual, provided a forged California driver's license to support the false identity, used the driver's license number from another person in support of the forged license, and provided a forged tax return to support his purported ability to pay rent. Defendant used the laptop he had procured through fraud in the apartment, and connected to the Internet with the aircard purchased with a false identity while using the account with Verizon that he maintained using a false identity. Even the electricity that lighted the apartment and powered the computer and aircard was purchased in a false name. What is more, while living in the apartment under false pretenses, Defendant had $70,000 in cash, a false passport, and a copy of his laptop computer in a storage unit (also rented under false pretenses) ready for a quick escape.
>
> Dkt. #1009, p. 9-10.

The Court made a series of manifest factual errors. *See* Section I, *supra*. Had the Court paid proper attention to the evidence and uncontested facts, the paragraph above would read as follows:

> Defendant rented the apartment using the name of a deceased individual, provided a forged California driver's license to support the false identity, ~~used the driver's license number from another person in support of the forged license,~~ and provided a forged tax return to support his purported ability to pay rent. Defendant used the laptop he had procured **using his own money** ~~through fraud~~ in the apartment, and connected to the Internet with the aircard purchased **with his own physical cash and while presenting no name at all** ~~a false identity~~ while using the account with Verizon that he maintained using a false identity. Even the electricity that lighted the apartment and powered the computer and aircard was purchased ~~in a false name~~ **under the same name as was used to rent the apartment**. What is more, while living in the apartment under false pretenses, Defendant had $70,000 in cash, a false passport, ~~and a copy of his laptop computer~~ in a storage unit (also rented under false pretenses) ~~ready for a quick escape~~.

The Court's attempt to multiply the purported "fraud"—which is really just simple "false pretenses" as the Court candidly admits—will not pass. The Court bolstering a finding of colloquial "fraud" via a fallacious presentation of the facts is manifest error. Evidence in support of the actual, uncontested facts—as used to edit the Court's paragraph above—is

contained in ¶¶ Nos. 1, 2, 3, 4 and 5, Section I, *supra*. As the record shows, the government failed to contest any of the defendant's declarations.

Additionally, the Court ignored the government's very clear concession that the "Defendant still had a reasonable expectation of privacy in the apartment itself..." *Government's Memorandum Regarding Law Enforcement Privilege And Request For An Ex Parte And In Camera Hearing If Necessary*, p. 22 fn. 3 (Dkt. #465, p. 22)

2. It was manifest error to find that the defendant was not "legitimately on the premises" under *Rakas* and *Jones*.

As noted above, the Court is relying upon what it describes as "false pretenses" to support its finding that the defendant had committed some sort of "fraud" and, therefore, was not "legitimately on the premises" while in his home residence and, therefore, had no reasonable expectation of privacy. A false representation, or "false pretense" as the Court puts it, is only one element of a fraud claim. "Under California law, the indispensable elements of a fraud claim include a false representation, knowledge of its falsity, intent to defraud, justifiable reliance, and damages." Fanucchi & Limi Farms v. United Agri Prods, 414 F.3d 1075, 1088 (9th Cir. 2005). It is clear from the record that the defendant had no intent to defraud Domicilio, Verizon, or Lenovo and no party can claim any type of damages. There is a gaping hole in the Court's "fraud" theory. The defendant did not have a "wrongful presence" in his home and he was certainly "legitimately on the premises" for each month he paid his rent using his own money. At most, there was breach of contract with no damages—but not "fraud"—which is addressed further in Section II(E)(5), *infra*.

However, if by "fraud" the Court means that some type of alleged criminal activity destroyed the defendant's reasonable expectation of privacy in his home, this theory also fails. *See*, *e.g.*, United States v. Pollock, 726 F.2d 1456, 1465 (9th Cir. 1984) (defendant who moved a laboratory to his friend's house to avoid detection and who used that site to manufacture drugs had a legitimate expectation of privacy).[79] The Court did note its

79. *See also* United States v. Skinner, ___ F.3d ___, No. 09-649, p. 7, fn. 1 (6th Cir., Aug. 14, 2012) ("We do not mean to suggest that there was no reasonable expectation of privacy *because* Skinner's phone was used in the commission of a crime, or that the cell phone was

personal opinion that the defendant "[h]aving utterly disregarded the privacy rights of Travis Rupard, Steven Brawner, and Andrew Johnson, not to mention the many other names used in his scheme, Defendant cannot now credibly argue that he had a legitimate expectation of privacy in the devices and apartment he acquired through the fraudulent use of their identities." Dkt. #1009, p. 13. It was entirely inappropriate for the Court to take into account his personal opinions regarding the criminal provisions the government asserts were violated. *See* United States v. Williams, 124 F.3d 411, 417 (3rd Cir. 1997) ("[I]n reviewing the issuance of a search warrant,... it does not follow that a judicial officer, in weighing the public interest, may properly take into account his or her personal opinions regarding the need for or the importance of the criminal provisions that appear to have been violated." (citations omitted)).

3. Even if the defendant was not "legitimately on the premises," it was manifest error for the Court to apply the *Jones* test as the *sole* test to determine reasonable expectation of privacy.

The Court stated that the Ninth Circuit in *Cunag* relied upon Rakas v. Illinois, 439 U.S. 128 (1978) to find that "when an individual is not legitimately on the premises, he does not enjoy the protection afforded by the Fourth Amendment." Dkt. #1009, p. 11 (*citing* United States v. Cunag, 386 F.3d 888, 893 (9th Cir. 2004)). The Court went on to acknowledge the Ninth Circuit's second finding in *Cunag*, which was based on *Bautista*,[80] *i.e.*, "one who procures a hotel room by fraud does have a reasonable expectation of privacy so long as the hotel has not taken affirmative steps to evict him." Dkt. #1009, p. 11 (*citing* Cunag, 386 F.3d at 895). However, the Court then found that "the Ninth Circuit had already concluded, under Supreme Court precedent, that Cunag was not lawfully in the room and therefore had no legitimate expectation of privacy, [therefore] the Court regards th[e *Bautista* reasoning] [] of *Cunag* as dicta." Dkt. #1009, p. 11. As explained below, the Court has it

---

illegally possessed."); United States v. Barajas-Avalos, 359 F.3d 1204, 1214 (9th Cir. 2004) (Interpreting *Sandoval* to hold that "a search of the interior of a makeshift tent violated the appellant's reasonable expectation of privacy even though he was camped illegally..." (citing Sandoval, 200 F.3d at 661)); United States v. Davis, 849 F.2d 414, 415 (9th Cir. 1988) ("We also reject the government's assertion that there is a contraband exception to the fourth amendment.").

80. United States v. Bautista, 362 F.3d 584 (9th Cir. 2004).

backwards. The actual dicta in *Cunag* is the quote from *Rakas* and the controlling law is the reasoning based on *Bautista*.

In the present case, the Court conducted a "legitimately on premises" test as the *sole* test when finding that the defendant had no reasonable expectation of privacy in his home. *See* Dkt. #1009, p. 9. In conducting this *sole* test, the Court found that the defendant's "presence in the apartment was wrongful" and stopped there. *Id*. This is where the Court made its mistake. The Supreme Court in *Rakas* did away with *solely* using the "legitimately on premises" test as established in Jones v. United States, 362 U.S. 257 (1960). The *Rakas* Court made clear that "the phrase 'legitimately on premises' coined in *Jones* creates too broad a gauge for measurement of Fourth Amendment rights." Rakas, 439 U.S. at 142. As further explained in *Rakas*, while "wrongful presence" can still be considered, it is **not** to be held as controlling:

> We would not wish to be understood as saying that legitimate presence on the premises is irrelevant to one's expectation of privacy, but it **cannot be deemed controlling**.
>
> Rakas, 439 U.S. at 148 (emphasis added).

Because the "legitimately on premises" test was held to **not** be controlling in *Rakas*, the actual dicta in *Cunag* was the statement that Cunag had no privacy interests simply because he was not "legitimately on the premises." The *Cunag* court understood the impropriety of this dicta and went on to analyze whether steps had been taken to evict Cunag from his room. It was manifest error for this Court to not also take these steps in the present case.

The Court's manifest error becomes even more evident in light of United States v. Young, 573 F.3d 711 (9th Cir. 2009). In *Young*, the Ninth Circuit agreed that "Young maintained a reasonable (although fraudulent) expectation of privacy in his hotel room and the luggage he left in the hotel room, because hotel staff **had not evicted him from the room**." *Id*. at 717 (emphasis added). The Ninth Circuit decided *Young* at least five years after *Cunag* and still applied what this Court regarded as "dicta."

4. When finding that the defendant was not "legitimately on the premises," it was manifest error for the Court to consider facts unknown to the agents as of the time of the search.

Even if this Court were to continue to ignore controlling Ninth Circuit precedent and find that the defendant fails the "legitimately on premises" test as the *sole* test, the defendant still had a reasonable expectation of privacy in his apartment. First, the Supreme Court made clear that "[t]he reasonableness of an official invasion of the citizen's privacy must be apprised on the basis of the facts **as they existed at the time that invasion occurred**." United States v. Jacobsen, 466 U.S. 109, 115 (1984) (emphasis added). In the context of using the StingRay and KingFish, the Court found that the "place [*i.e.*, real property] to be searched could not be specified because it was unknown..." Dkt. #1009, p. 29. Therefore, all the so-called "fraud" relied upon by the Court to find that the defendant was not "legitimately on the premises" cannot be considered. At the time the invasion occurred, Jacobsen, 466 U.S. at 115, the government had no information regarding the defendant renting his apartment and paying his electricity under the name of Steven Brawner. Just as the Ninth Circuit found in *Young*, this defendant still had a reasonable expectation of privacy **even if** there was "fraud" and **even if** the defendant was not "legitimately on the premises" considering those facts came to light after the government invasion:

> *Cunag* involved a defendant who had been conclusively evicted from his hotel room after hotel management confirmed that the room had been procured through credit card fraud. The lockout was done with the clear intention of permanently removing Cunag from the room, as demonstrated by the simultaneous filing of the crime report with the police. Here, hotel management was **unaware of the possibility that Young had procured the room through fraud**.
>
> Young, 573 F.3d at 719 (emphasis added) (distinguishing *Cunag*).

5. The Court's manifest error in finding that the the defendant was not "legitimately on premises" based on breach of contract has the potential to bread tyrannical government misconduct.

If applied liberally by government investigators and prosecutors, the tyranny that could potentially result from the Court's ruling addressing the defendant's reasonable expectation of privacy is saddening. In an attempt to distinguish controlling Ninth Circuit case law, the Court partially relied upon United States v. Johnson, 584 F.3d 995 (10th Cir.

2009), as well as similar out-of-circuit cases. *See* Dkt. #1009, p. 12. In *Johnson*, the Tenth Circuit found that a defendant had no reasonable expectation of privacy in a storage unit because the renter violated the rental agreement by entering into the contract using a false name. *See id*. The Tenth Circuit applied Utah contract law and found that the agreement "was a contract voidable at the storage unit owner's option. At all times, then, [][the renter's] contractual right to the storage unit was in jeopardy of recession." *Id.* at 1004. Based on this breach of contract, the *Johnson* court found there was no reasonable expectation of privacy in the storage unit. *See Id*. Just like Domicilio of whom the defendant rented his home, the storage facility in *Johnson* was **not** defrauded of anything of value, which is a required element of "fraud."[81] Therefore, the "fraud" theory upon which this Court basis its decision is more appropriately categorized as "breach of contract." At most, the defendant breached the leasing contract he had with the Domicilio apartment complex by using a false name.[82] It was this breach of contract that the Court based its finding that the defendant's "presence in the apartment was wrongful[.]" Dkt. #1009, p. 9. As explained below, finding that a person had no reasonable expectation of privacy in a rented home simply because there was a violation of the lease will only further tyrannical government misconduct.

The *Johnson* court's theory of contract law controlling one's reasonable expectation of privacy has repeatedly been rejected by the Supreme Court in the context of **home residences**. "In defining the scope of that interest, we adhere to the view expressed in *Jones* and echoed in later cases that arcane distinctions developed in property and tort law between guests, licensees, invitees, and the like, ought not to control." Rakas, 439 U.S. at 143 (listing cases). This is sound legal reasoning. Otherwise, law enforcement could justify an illegal search and seizure, after the fact, by pointing to any violation of a leasing contract to establish that a defendant's "presence... was wrongful" while inside his home. Dkt. #1009, p. 9. For example, a prosecutor can now show a lack of privacy expectations because of

---

81. The words "to defraud" usually signify the deprivation of something of value by trick, deceit, chicane, or overreaching. *See* McNally v. United States, 483 U.S. 350, 358 (1987).

82. The *pro se*, incarcerated defendant does not have access to California contract law resources. Therefore, the defendant does not concede that entering into a contract using an alias is breach of contract in California.

Sparky, the household pet goldfish. "After all, your Honor, the defendant's presence in the leased apartment was wrongful considering the leasing contract clearly forbids fishtanks of any kind." As another example, federal agents could measure a resident's hedges to see if they comply with height requirements established by the Home Owner's Association. "Your Honor, the defendant was wrongfully on the premises. His hedges had not been cut for what we estimate to be six months. Because this 'fraud' upon his neighbors was a clear violation of the home owner's agreement, there was no reasonable expectation of privacy." The Court may dismiss the defendant's concerns as puffery. But, "[t]he difference between puffery and prosecution may depend on whether you happen to be someone an AUSA has reason to go after." United States v. Nosal, 676 F.3d 854, 862 (9th Cir. 2012). "[W]e shouldn't have to live at the mercy of our local prosecutor.... By giving that much power to prosecutors, we're inviting discriminatory and arbitrary enforcement." *Id*.

6. Even if the defendant had no reasonable expectation of privacy in his home residence, he still had a possessory and property interest in his aircard and computer.

In its order, the Court found the following:

> Citing *Lavan v. City of Los Angeles*, 693 F.3d 1022 (9th Cit. 2012), Defendant asserted at oral argument that he need not show a reasonable expectation of privacy to make out a Fourth Amendment violation because the Fourth Amendment also protects property interests, and he had a property interest in his apartment, laptop, and aircard. *Lavan* did not concern a search, but instead concerned the City's seizure and destruction of personal property belonging to homeless people that was left on City sidewalks. In addition, for the reasons discussed above, the Court cannot conclude that Defendant had a legitimate Fourth Amendment property interest in the apartment, laptop, or aircard procured through fraud.
>
> Dkt. #1009, p. 14 fn. No. 3.

First, the defendant made the same seizure arguments at Dkt. #824-1. The defendant identified conceded Fourth Amendment seizures conducted by the government under United States v. Jacobsen, 466 U.S. 109, 113 (1984) and under Soldal v. Cook County, 506 U.S. 56, 61 (1992). The defendant also identified conceded Fourth Amendment searches that involved trespassing to obtain information under United States v. Jones, 556 U.S. ___, 181 L. Ed. 2D 911 (2012), which do not require a reasonable expectation of privacy.

Second, the Court erred by only analyzing property interests and not possessory interests. The Supreme Court made clear in *Jacobsen* that "A 'seizure' of property occurs when there is some meaningful interference with an individual's **possessory interests** in that property." *Id.* at 113 (emphasis added). The government already conceded that the defendant had possessory interests. *See Government's Response To Defendant's Motion To Suppress* (Dkt. #873, p. 60) (The government agreed that the defendant "personally possessed, obtained, or maintained the items."). Therefore, the defendant has the requisite "standing" to challenged the conceded Fourth Amendment searches and seizures classified under *Jacobsen*, *Soldal*, and *Jones*.

Third, the defendant had legitimate ownership of his aircard and laptop computer. As noted in Section I, *supra*, ¶ No. 4, the defendant purchased his aircard using his **own physical cash while providing no name at all** and the laptop was also purchased with the defendant's own money. The government does not contest these facts. Additionally, the aircard and laptop were not connected to Verizon Wireless while the FBI was operating the StingRay and KingFish. Therefore, the Travis Rupard Verizon Wireless account holds no relevancy to any property, possessory, or privacy interests. As for legitimate property interests, if the defendant did not own the aircard and laptop then who did? Furthermore, even if those items were owned by someone else, they were in the defendant's possession and this "raise[s] the questions at issue in cases where a guest is still using a room that he obtained by fraudulent use of a credit card." Caymen, 404 F.3d at 1199 (footnote omitted) (citing United States v. Cunag, 386 F.3d 888 (9th Cir. 2004); United States v. Bautista, 362 F.3d 584 (9th Cir. 2004)). It was manifest error for the Court to ignore these points.

I. It was manifest error for the Court to completely ignore the defendant's arguments relating to the N.D.Cal. 08-90331MISC-RS Pen/Trap oder used to force the aircard to generate real-time cell site information.

At Dkt. #824-1, the defendant raised numerous challenges to the N.D.Cal. 08-90331MISC-RS oder used to justify use of the SF-Martinez DCS-3000 Pen/Trap device. It was manifest error for the Court to ignore every single one of those arguments.

J. It was manifest error for the Court to completely ignore the defendant's arguments contained in Memorandum RE: Destruction Of Evidence In Support Of: Motion To Suppress (Dkt. #830-2).

At Dkt. #830-2, the defendant asked for suppression of evidence as a sanction for the government's destruction of evidence relating to all data obtained from Verizon Wireless under the purported execution of the N.D.Cal. 08-90330MISC-RS order. The memorandum relates to data that was purportedly obtained separate from use of the FBI's cell site emulators. It was manifest error for the Court to ignore the memorandum.

III. Modifications Of The Order Being Sought

The defendant requests that the Court ***(1)*** reevaluate all aspects of its order in light of the corrected facts contained in Section I, *supra*, ***(2)*** address the argument regarding the N.D.Cal. 08-90330MISC-RS order never having been executed, *see* Section II(A), *supra*, ***(3)*** address the defendant's scope arguments relating to the independent Fourth Amendment searches and seizures conceded by the government on January 27, 2012, *see* Section II(B), (1) and (2), *supra*, ***(4)*** address the scope argument relating the government only receiving authorization to use one "mobile tracking device," as opposed to two, *see* Section II(C), *supra*, ***(5)*** address the defendant's argument regarding the N.D.Cal. 08-90330MISC-RS order not commanding the use of any "mobile tracking device" in the operative section of the order, *see* Section II(D), *supra*, ***(6)*** reevaluate the defendant's argument regarding the government failing to explain new surveillance technology in light of the *Oliva* Ninth Circuit decision, *see* Section II(E), *supra*, ***(7)*** reevaluate the decision to consider the unincorporated and unaccompanied application and affidavit for the N.D.Cal 08-90330MISC-RS order, *see* Section II(F), *supra*, ***(8)*** reevaluate/address the defendant's arguments raised regarding the digital data search, *see* Section II(G), (1), (2), (3), (4) and (5), *supra*, ***(9)*** reevaluate the finding that the defendant lacked a reasonable expectation of privacy, *etc*. in his home and possessions, *see* Section II(H), (1), (2), (3), (4), (5), and (6), *supra*, ***(10)*** address the sections of the defendant's briefs that were entirely ignored by the Court at Dkt. #1009, *see* Section II(I) and (J), *supra*, and ***(11)*** suppress all evidence resulting from the government's searches and seizures.

* * * * *

This filing was drafted by the *pro se* defendant, however, he authorizes his shadow counsel, Philip Seplow, to file this filing on his behalf using the ECF system.

LRCrim 12.2(a) requires the following text in motions: "Excludable delay under 18 U.S.C. § 3161(h)(1)(D) will occur as a result of this motion or of an order based thereon."

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

Respectfully Submitted: May 22, 2013

PHILP SEPLOW, Shadow Counsel, on behalf of DANIEL DAVID RIGMAIDEN, Pro Se Defendant:

s/ Philip Seplow
Philip Seplow
Shadow Counsel for Defendant.

CERTIFICATE OF SERVICE

I hereby certify that on: May 22, 2013 I caused the attached document to be electronically transmitted to the Clerk's Office using the ECF system for filing and transmittal of a Notice of Electronic Filing to the following ECF registrants:

Taylor W. Fox, PC
Counsel for defendant Ransom Carter
2 North Central Ave., Suite 735
Phoenix, AZ 85004

Frederick A. Battista
Assistant United States Attorney
Two Renaissance Square
40 North Central Ave., Suite 1200
Phoenix, AZ 85004

Peter S. Sexton
Assistant United States Attorney
Two Renaissance Square
40 North Central Ave., Suite 1200
Phoenix, AZ 85004

James R. Knapp
Assistant United States Attorney
Two Renaissance Square
40 North Central Ave., Suite 1200
Phoenix, AZ 85004

By: s/ Daniel Colmerauer
(Authorized agent of Philip A. Seplow, Shadow Counsel for Defendant; See ECF Proc. I(D) and II(D)(3))